Jason Patrick, Pro Se
c/o Andrew M. Kohlmetz, OSB #955418
Kohlmetz Steen & Hanrahan PC
741 SW Lincoln Street
Portland, OR 97201
Tel: (503) 224-1104
Fax: (503) 224-9417
Email: andy@kshlawyers.com

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. JASON PATRICK, Defendant	Case No. 3:16-CR-00051-BR-09 DEFENDANT'S MEMORANDUM IN SUPPORT OF MOTION TO COMPEL PRODUCTION OF INFORMATION PERTAINING TO DEFENDANTS AND WITNESSES CONTAINED WITHIN VARIOUS LAW ENFORCEMENT DATABASES

Mr. Patrick, on behalf of all defendants submits the following Memorandum describing the databases from which the requested information is sought and why the information sought is discoverable.

A: The Information Sought is Relevant to This Case

1: Information gleaned by investigators from these databases is referenced in law enforcement applications for warrants and court orders.

By way of example, in reviewing discovery materials related to a Search Warrant for Geolocation Data for a phone linked to Mr. Patrick, an FBI 302 was found that indicates "Guardian lead 300157_SE" was used in the creation of the affidavit sworn out in support of the Warrant (Discovery at Bates MNWR_0003077). Review of the referenced affidavit however yields no reference to any such "Guardian lead." (Discovery at Bates range MNWR_0000219-233). Defendant needs to know what this Guardian lead was and how, or even if, it was in fact

Kohlmetz Steen & Hanrahan PC
741 SW Lincoln Street
Portland, OR 97201
(503) 224-1104

incorporate into this affidavit. Moreover, the "lead" most certainly did not exist in a vacuum and begs the question what other information pertaining to Mr. Patrick was contained within the Guardian system that might provide additional context or have some bearing on the Affidavit? As the defendants continue to prepare for trial, the bases of factual assertions contained within various government affidavits and applications must be disclosed to the defense in order that they be evaluated to determine whether or not Motions to Suppress or Controvert are appropriate. More generally, these databases – particularly eGuardian/DIVS – have been noted by the FBI to raise serious First and Fourth Amendment implications. Discovery of the requested materials is necessary to analyze whether any information within the databases themselves, or the manner in which it was collected, violates any of the defendants' rights under the First or Fourth Amendment, thereby potentially leading to "fruit of the poisonous tree" derivative suppression motions related to subsequent investigation results and or pleadings.

2: Information in government databases about government witnesses will constitute relevant impeachment evidence.

Within the discovery these databases are routinely referenced as having been searched in FBI reports documenting contacts, tips, and interviews with witnesses. According to publicly available information on these databases and the information they are designed to contain it is highly likely that relevant and/or impeachment evidence exists within these databases as to many of the defendants and potential witnesses in this case. FBI reports documenting database inquiries note the presence or lack of "derogatory information" within the database(s) searched.

3: Information in government databases concerning the activities, statements, motivations and associations of these defendants is likely to be admissible, or at least lead to admissible evidence.

In Count One, the government has charged these defendants with Conspiracy to Impede Federal Officers by Force, Threat or Intimidation. The heart of the charge is the alleged conspiratorial agreement. Countering the charge will necessarily involve an attempt at negating the element of a criminal agreement to impede. The alleged mental states, and motivations of these defendants will be central to both the government and the defense case herein. From the publicly available descriptions of these databases it appears highly likely they will contain

Kohlmetz Steen & Hanrahan PC
741 SW Lincoln Street
Portland, OR 97201
(503) 224-1104

evidence relevant to the case. The discovery is replete with FBI references to various defendants' involvement with "militia type" groups. Based on publicly available documents, it appears that the FBI, has conducted full "enterprise" investigations into these groups.[1] Any such investigations would likely yield valuable evidence of group-members historical and current motivations and goals, as well as identifying additional persons with knowledge of such.

B: General Information Concerning the Databases:

In 2007 the federal government developed the Nationwide Suspicious Activity Reporting Initiative commonly referred to as "NSI."[2] THE NSI established a nationwide system for various law enforcement agencies at local, state, tribal and federal level to gather and share Suspicious Activity Reports (SAR) that have a potential nexus to terrorism or other criminal activity." *Id.* One of the primary systems used to collect, share, investigate and analyze SARs is the FBI's eGuardian system. *Id at p. 3*. DOJ is charged with managing the NSI and the FBI leads the effort to implement the NSI. *Id at p. 6.* In addition to eGuardian, the FBI has access to and regularly relies upon a number of other databases in its criminal investigations. These databases contain a tremendous amount of data on included individuals and groups.

In 2008 the Department of Justice issued The Attorney General's Guidelines for Domestic FBI Operations.[3] This document represented the "…culmination of the historical evolution of the FBI and the policies governing its domestic operations…" after the terrorist attacks of 9-11. This evolution transformed the FBI into a domestic intelligence as well as a domestic law enforcement agency. Criminal intelligence gathering and analysis is now a core

---

[1] According to the Attorney General's Guidelines for Domestic Operations, see fn 3 below, An FBI "Enterprise Investigation" is a full investigation of a group or organization based on a reasonable indication that the group may be engaged in domestic terrorism or other violations of federal law. The scope of such investigations are broad and includes examinations of the group's members, relationships, history, plans and goals. Partial NCIC records already provided in discovery indicate that these defendants are on a "terrorist watchlist."

[2] United States Government Accountability Office ("GAO") Report to Congressional Requesters, GAO-13-233, March 26, 2013: United States Government Accountability Office (GAO) Report to Congressional Requesters, GAO-13-233, p. 1, March 26, 2013: http://www.gao.gov/products/GAO-13-233

[3] https://www.justice.gov/sites/default/files/ag/legacy/2008/10/03/guidelines.pdf

Kohlmetz Steen & Hanrahan PC
741 SW Lincoln Street
Portland, OR 97201
(503) 224-1104

mission of the FBI. In an effort to meet the goals of its intelligence gathering mission the FBI has increasingly utilized its own electronic information databases as both investigation and intelligence tools. In a very real sense the FBI has embarked on a vigorous campaign of domestic surveillance. Entry of an individual's personal information into the system can be initiated from any source and on the barest hint of "suspicious activity." These domestic surveillance tools were actively brought to bear in this case. The databases so far identified in the discovery are briefly described below:

SENTINEL[4]

SENTINEL is the FBI's electronic case file management system which documents cases from inception to closure. While its primary purpose is case management, SENTINEL does provide case search and analytical capabilities. SENTINEL is a term-searchable database and can be used to "identify connections between cases and patterns of activity." SENTINEL is also designed to share case file information with other databases, specifically DIVS. DIVS, and other data warehouse systems like it allow FBI and other authorized law enforcement personnel to undertake simultaneous searches of multiple searchable electronic resources and databases. This cross platform functionality may "reveal previously unknown relationships among individuals and groups under investigation."

The FBI has publicly identified concerns that the SENTINEL system may collect too much personal information concerning those it targets, and that much of the information so collected will be either inaccurate or irrelevant.

Guardian and eGuardian[5]

The Guardian program is an FBI designed program to facilitate the sharing of law enforcement investigatory information between local, state and federal law enforcement agencies. It has two components; a classified system which resides on FBI networks (called

[4] Information in this section taken from the FBI's Privacy Impact Assessment for the Sentinel System dated May 28, 2014, located at https://www.fbi.gov/foia/privacy-impact-assessments/sentinel

[5] Information in this section taken from the FBI's Privacy Impact Assessment for the eGuardian System dated January 4, 2013, located at https://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat

Kohlmetz Steen & Hanrahan PC
741 SW Lincoln Street
Portland, OR 97201
(503) 224-1104

Guardian) and its unclassified version which is made available to law enforcement agencies down to the local and tribal level. (called eGuardian). The eGuardian system is designed to collect a wide variety of information from broad terrorist threats down to local "suspicious activity." "Suspicious activity" is defined as observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. To be entered as possible criminal activity, the information must be based upon "a reasonable suspicion an activity constituting a federal crime or a threat to national security has or may have occurred, is or may be occurring, or will or may occur." Information entered by law enforcement agencies into the system can come from any source private or governmental.

The FBI recognizes the program presents a risk that the collection of such a broad amount of data has constitutional implications. For example, FBI Guidelines prohibit the collection of information based solely on the exercise of First Amendment rights. In analyzing Fourth Amendment privacy concerns, the FBI notes:

> The most significant privacy risk is that the collected information, upon further vetting, is deemed to be innocuous, resulting in the overcollection of data.
>
> Another privacy risk is the sum of the data entered into the eGuardian system may be greater than its component parts, with the result that new and different information about incidents and people alleged to be suspicious becomes apparent. This is, in significant part, the purpose of the eGuardian system, but it also creates a privacy risk and a risk of public misperception and possible misunderstanding. The privacy risk is that seemingly isolated incidents or observations may lead to more discovery of personal information about individuals in an effort to develop relationships (i.e., "connect the dots") between these and other incidents and observations.

DIVS[6]

DIVS, or Digital Integration and Visualization System is described in 2011 by the FBI as a "new tool which encompasses the Bureau's most-used databases while providing a single-source search capability that pulls information directly from hundreds of databases and data

[6] Information in this section taken from an FBI Press Release dated March 9, 2011, located here https://www.fbi.gov/about-us/itb/news-features/new-database-search-tool-will-aid-bureau-investigations

Kohlmetz Steen & Hanrahan PC
741 SW Lincoln Street
Portland, OR 97201
(503) 224-1104

sets." FBI statements about DIVS make clear that it is a warehouse of electronic information combined from a multitude of sources. According to publicly released budgeting documents about DIVS:

> The FBI DIVS program stores and presents for analysis the FBI's intercepted electronic surveillance (ELSUR) data authorized for collection under the Foreign Intelligence Surveillance Act (PISA) and electronic data obtained from seized or captured digital media. The resulting system will enable agents, analysts, and linguists to analyze data obtained by different methods using a single tool set, thus reducing training requirements as well as enable more efficient and effective analysis of all stored data holdings.[7]

There is no publicly available Privacy Impact Assessment for the DIVS system. However, the nature of the DIVS system gives rise to the same First and Fourth Amendment concerns identified by the FBI in its own privacy assessment of the eGuardian and SENTINEL systems.

ORION[8]

The Operational Response and Investigative Online Network (ORION) is described in publicly available documents as responsive, real time investigatory database that is at least in-part autonomously processing, analyzing and disseminating investigative information. It is described as a real-time online network designed to coordinate law enforcement efforts in crisis situations. ORION also has the ability to autonomously analyze and compare data as it is entered into the system and make case associations and "push leads and intelligence" to other investigators. In addition to the same First and Fourth Amendment concerns as presented by both the Guardian and DIVS systems, ORION introduces another dimension in that it is a reactionary crisis base system which has automated some of the report entry and analysis functions. It appears designed for speed and not accuracy. Software driven automated investigatory tools raise in this context fundamental constitutional concerns.

---

[7] https://www.justice.gov/sites/default/files/jmd/legacy/2014/08/11/fbi-2011-divs.pdf

[8] Information in this section taken from an FBI Press release dated September 22, 2008 located here https://www.fbi.gov/news/stories/2008/september/orion_092208

Kohlmetz Steen & Hanrahan PC
741 SW Lincoln Street
Portland, OR 97201
(503) 224-1104

NGI-IPS[9]

The Next Generation Identification – Interstate Photo System of NGI-IPS is an FBI database that provides for text based and facial recognition search capabilities for individuals' civil and criminal biometric data (fingerprints, personal data, employment data etc.) and photographs. Law enforcement personnel can submit photographs of suspects for identification into the system. The system, through facial recognition software will then automatically produce a list of identified potential candidates. Because of the inherent limitations of the current generation of facial recognition software, the FBI has identified the system's potential for erroneous identifications.

> The retention of more criminal photos and the searching and dissemination of these photos based on face recognition technology poses a risk of erroneous identification of the subject of the photo. More specifically, face recognition searching of Criminal Identity Group photos could include the risk that the technology may not be sufficiently reliable to accurately locate other photos of the same identity, resulting in an increased percentage of misidentifications.

While there is only one reference of which defendant is aware in the discovery that the NGI-IPS was used in this case, various defendants have raised claims during the course of these proceedings that they were the subject of a "misidentification." To the extent NGI-IPS contains any of the requested material, it is included herein.

NCIC

Routinely provided as discovery in this District are National Crime Information Center (NCIC) records. According to publicly available sources, the NCIC database is "the lifeline of law enforcement."[10] It has been in use since 1967 and currently contains over 12 million active records. The system currently averages over 12.6 million transactions every day. NCIC printouts have been provided in discovery for at least some of the defendants herein.

---

[9] Information in the section taken from the FBI's Privacy Impact Assessment for the NGI-IPS system dated September 2015, located https://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system

[10] https://www.fbi.gov/about-us/cjis/ncic

Kohlmetz Steen & Hanrahan PC
741 SW Lincoln Street
Portland, OR 97201
(503) 224-1104

C: Legal Argument

1. **The Information Sought is Discoverable Under F.R.Cr.P. 16**

Federal Rule of Criminal Procedure 16 grants the accused a "broad right" to discovery. *United States v. Stever*, 603 F3d 747, 752 (9th Cir. 2010). The government must produce all documents within its possession, custody or control that are material to the defense. Id. The government is in possession of any documents of which it has knowledge and access. *United States v. Santiago*, 46 F.3d 885, 893 (9th Cir.1995). This includes information in the possession of all law enforcement agencies involved in the case. *United States v. Bryan*, 868 F.2d 1032, (9th Cir. 1989), *and United States v. Santiago*, 46 F.3d 885, 893-94 (9th Cir. 1995)(Knowledge and access test the proper tool to determine the "scope" of government's discovery obligation.) To show materiality under this rule the defendant must demonstrate that the requested evidence "'bears some abstract logical relationship to the issues in the case . . . . There must be some indication that the pretrial disclosure of the disputed evidence would [enable] the defendant significantly to alter the quantum of proof in his favor.'" *United States v. Lloyd*, 992 F.2d 348, 350-51 (D.C. Cir. 1993)(citations omitted). This materiality standard normally "is not a heavy burden"; rather, "evidence is material as long as there is a strong indication that it will 'play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal.' " *Id.*

2. **The information sought is Brady material**

Under *Brady*, the government must disclose to the defendant all "favorable" evidence that is "material either to guilt or to punishment." *Brady v. Maryland, 373 U.S. 83, 87, 83 S.Ct. 1194, 10 L.Ed.2d 215 (1963).* Evidence is favorable and material if it would "tend to exculpate" the defendant or "reduce the penalty". *Id.* As the Ninth Circuit has noted, the *Brady* rule is to be construed liberally;

> [T]he proper test for pretrial disclosure of exculpatory evidence should be an evaluation of whether the evidence is favorable to the defense, i.e., whether it is evidence that helps bolster the defense case or impeach the prosecutor's witnesses…[I]f doubt exists, it should be resolved in favor of the defendant and full disclosure made… [T]he government [should therefore] disclose all evidence relating to guilt or punishment which might reasonably

Kohlmetz Steen & Hanrahan PC
741 SW Lincoln Street
Portland, OR 97201
(503) 224-1104

> be considered favorable to the defendant's case, even if the evidence is not admissible so long as itis reasonably likely to lead to admissible evidence.

United States v. Price, 566 F.3d 900, 913 (9th Cir. 2009) *quoting, United States v. Acosta,* 357 F. Supp.2d 1228, 1239-40 (D.Nev. 2005) *citing, United States v. Sudikoff,* 36 F. Supp.2d 1196 (C.D.Cal 1999.) Under *Brady*, there is no distinction between exculpatory and impeachment evidence. *United States v. Bagley, 473 U.S. 667, 682, 105 S.Ct. 3375, 87 L.Ed.2d 481 (1985).* Favorable evidence is material evidence and "…evidence that would impeach a central prosecution witness is indisputably favorable to the accused. *United States v. Price, 566 F.3rd at 907, citing Giglio v. United States, 405 U.S. 150, 154, 92 S.Ct. 763, 31 L.Ed.2d 104 (1972)(further citations omitted.)*

3. Department of Justice Policy Confirms The Requested Materials are Discoverable.

The Current United States Attorneys' Criminal Resource Manual states plainly that prosecutors must affirmatively seek out all exculpatory and impeachment information from federal, state, and local law enforcement agencies participating in the investigation and prosecution.[11] Prosecutors are directed to review the entire file of any agency involved in the case. The use by case agents of select information contained in these various databases in the investigation and prosecution of these defendants places the entirety of the information they contain within the ambit of the government's discovery and *Brady* obligations herein.

D: Conclusion:

Quite beyond the fact that the government is in possession of this information and that it should be produced under Rule 16 and/or as exculpatory information under Brady, are the Fourth Amendment implications of the FBI's transformation into a domestic surveillance and intelligence gathering agency. The sheer scope of the information contained within these databases and the variety of sources (public, private, law enforcement etc.) give rise to serious constitutional concerns. While the collection of any particular data points or sets from public sources may be unobjectionable, the effect of amalgamating so much data with the government's

[11] https://www.justice.gov/usam/criminal-resource-manual-165-guidance-prosecutors-regarding-criminal-discovery

Kohlmetz Steen & Hanrahan PC
741 SW Lincoln Street
Portland, OR 97201
(503) 224-1104

own law enforcement investigative data, is a new phenomenon. Fourth Amendment jurisprudence is only now beginning to address the argument that an individual's right to privacy in electronically stored data is a multi-faceted and nuanced concept. As Justice Sotomayor recently wrote in her concurrence in *United States v. Jones*, it may be time to reevaluate the way in which our government utilizes its ability to collect and analyze data about its citizens.

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. …
>
> I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. See *Smith*, 442 U.S., at 749, 99 S.Ct. 2577 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also *Katz*, 389 U.S., at 351–352, 88 S.Ct. 507 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

United States v. Jones, 132 S. Ct. 945, 957, 181 L. Ed. 2d 911 (2012)(Sotomayor, J. concurring).

The FBI's utilization of powerful electronic databases that combine massive quantities of data both private and public in its intelligence and investigative capacities in this case give rise to demonstrable concerns that these defendants' Fourth Amendment rights have been impacted. The requested material should be produced.

RESPECTFULLY SUBMITTED This 29th day of June, 2016.

Jason Patrick

Jason Patrick, Pro Se

Kohlmetz Steen & Hanrahan PC
741 SW Lincoln Street
Portland, OR 97201
(503) 224-1104